

B'
A
con

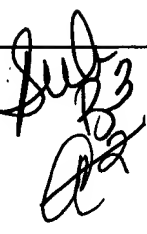
- 8 b) establishing a first stream between the first process and the communication
- 9 channel;
- 10 c) establishing a second stream between the second process and the
- 11 communication channel;
- 12 d) encrypting data to be transmitted between the first and second processes, the
- 13 encrypting of the data being independent of the at least one communication
- 14 protocol supported by the first and second network [node;] nodes;
- 15 e) writing the encrypted data to the first stream;
- 16 f) causing the encrypted data to be transmitted from the first network node to
- 17 the second network [node;] node according to the at least one communication
- 18 protocol supported by the first and second network nodes;
- 19 g) reading the encrypted data from the second stream; and
- 20 h) decrypting the encrypted data to obtain decrypted data which is identical to
- 21 the data on the first network node before the data was encrypted.

- 1 2. (Unamended) The method of Claim 1, further including the steps of
- 2 a) performing a communication protocol-specific encryption of the data on the
- 3 first network node, and
- 4 b) performing a communication protocol-specific decryption of the data on the
- 5 second network node.

- 1 3. (Unamended) The method of Claim 1, wherein the communication channel is a Java
- 2 secure channel,
- 3 wherein the first stream is a first Java stream,
- 4 wherein the second stream is a second Java stream,

5 wherein the step of establishing a communication channel between the first and
6 second network nodes further comprises the step of establishing a Java secure
7 channel between the first and second network nodes,
8 wherein the step of establishing a first stream between the first process and the
9 communication channel further comprises the step of establishing a first Java
10 stream between the first process and the Java secure channel,
11 wherein the step of establishing a second stream between the second process and the
12 communication channel further comprises the step of establishing a second
13 Java stream between the second process and the Java secure channel,
14 wherein the step of writing the encrypted data to the first stream further comprises
15 the step of writing the encrypted data to the first Java stream, and
16 wherein the step of reading the encrypted data from the second stream further
17 comprises the step of reading the encrypted data from the second Java stream.

1 4. (Unamended) The method of Claim 1, wherein the communication channel is a Java
2 secure channel, wherein the first stream is a Java stream,
3 wherein the second stream is a Java stream,
4 wherein the method further comprises the step of connecting the Java secure channel
5 to a third Java stream, and
6 wherein the third Java stream provides for the transmission of data according to a
7 specific communication protocol.

 1 5. (Amended) A computer-readable medium [having stored thereon a plurality of
2 sequences of] carrying one or more sequences of one or more instructions for
3 providing communication protocol-independent security for data transmitted between
4 a first process, executing on a first network node, and a second process, executing on
5 a second network node, wherein the first network node and the second network node

B3
A2
cont

6 each support at least one common communication protocol, the [plurality of] one or
7 more sequences of one or more instructions including [sequences of] instructions
8 which, when executed by one or more processors, cause the one or more processors
9 to perform the steps of:

- 10 a) establishing a communication channel between the first network node and the
11 second network node;
12 b) establishing a first stream between the first process and the communication
13 channel;
14 c) establishing a second stream between the second process and the
15 communication channel;
16 d) encrypting data to be transmitted between the first and second processes, the
17 encrypting of the data being independent of the at least one common
18 communication [protocols] protocol supported by the first and second
19 network [node;] nodes;
20 e) writing the encrypted data to the first stream;
21 f) causing the encrypted data to be transmitted from the first network node to
22 the second network [node;] node according to the at least one communication
23 protocol supported by the first and second network nodes;
24 g) reading the encrypted data from the second stream; and
25 h) decrypting the encrypted data to obtain decrypted data which is identical to
26 the data on the first network node before the data was encrypted.

- 1 6. (Unamended) The computer-readable medium of Claim 5, wherein the computer-
2 readable medium further includes instructions for performing the steps of
3 a) performing a communication protocol-specific encryption of the data on the
4 first network node, and

5 b) performing a communication protocol-specific decryption of the data on the
6 second network node.

1 7. (Unamended) The computer-readable medium of Claim 5, wherein the first stream is
2 a first Java stream,
3 wherein the second stream is a second Java stream,
4 wherein the step of establishing a communication channel between the first and
5 second network nodes further comprises the step of establishing a Java secure
6 channel between the first and second network nodes,
7 wherein the step of establishing a first stream between the first process and the
8 communication channel further comprises the step of establishing a first Java
9 stream between the first process and the Java secure channel,
10 wherein the step of establishing a second stream between the second process and the
11 communication channel further comprises the step of establishing a second
12 Java stream between the second process and the Java secure channel,
13 wherein the step of writing the encrypted data to the first stream further comprises
14 the step of writing the encrypted data to the first Java stream, and
15 wherein the step of reading the encrypted data from the second stream further
16 comprises the step of reading the encrypted data from the second Java stream.

1 8. (Unamended) The computer-readable medium of Claim 5, wherein the
2 communication channel is a Java secure channel,
3 wherein the first stream is a Java stream,
4 wherein the second stream is a Java stream,
5 wherein the computer-readable medium further includes instructions for connecting
6 the Java secure channel to a third Java stream, and

7 wherein the third Java stream provides for the transmission of data according to a
8 specific communication protocol.

1 9. (Amended) A communication network providing communication protocol-
2 independent secure communication between a first network node and a second
3 network node, wherein the first network node and the second network node each
4 support at least one common communication protocol, wherein the first network
5 node is communicatively coupled to the second network node by a communication
6 channel, the communication network comprising:
7 a) a first process executing on the first network node, wherein the first process is
8 configured to provide for the [provides for the communication protocol-
9 independent] encryption of [data;] data independent of the at least one
10 communication protocol;
11 b) a first stream which provides for the transfer of encrypted data between the
12 first process and the communication channel;
13 c) a second process executing on the second network node; and
14 d) a second stream which provides for the transfer of encrypted data between the
15 communication channel and the second process, wherein the second process
16 is configured to provide [also provides] for the decryption of data which has
17 been encrypted by the first process.

1 10. (Unamended) The communication network of Claim 9, wherein the second process
2 further includes the capability to decrypt data based upon any communication
3 protocol supported by the second network node.

1 11. (Unamended) The communication network of Claim 9, wherein the communication
2 channel is a Java secure channel, the first stream is a Java stream and the second
3 stream is a Java stream

1 12. (Unamended) The communication network of Claim 11, further comprising a third
2 Java stream connected to the Java secure channel, the third Java stream providing for
3 the transmission of data according to a specific communication protocol.

Sub
B5
A4
1 13. (Amended) A computer data signal embodied in a carrier wave and representing
2 sequences of instruction which, when executed by one or more processors, provide
3 communication protocol-independent security for data transmitted between a first
4 process, executing on a first network node, and a second process, executing on a
5 second network node, [wherein the first network node and the second network node
6 each support] according to at least one common communication protocol supported
7 by the first and second network nodes, by performing the steps of:
8 a) establishing a communication channel between the first network node and the
9 second network node;
10 b) establishing a first stream between the first process and the communication
11 channel;
12 c) establishing a second stream between the second process and the
13 communication channel;
14 d) encrypting data to be transmitted between the first and second processes, the
15 encrypting of the data being independent of the at least one common
16 communication [protocols] protocol supported by the first and second
17 network [node;] nodes;
18 e) writing the encrypted data to the first stream;

- B5
19
20
21
22
23
24
- Q4
Con 24
- f) causing the encrypted data to be transmitted from the first network node to the second network [node;] node according to the at least one common communication protocol;
- g) reading the encrypted data from the second stream; and
- h) decrypting the encrypted data to obtain decrypted data which is identical to the data on the first network node before the data was encrypted.

1 14. (Unamended) The computer data signal of Claim 13, wherein the computer
2 sequence of instructions further includes instructions for performing the steps of
3 a) performing a communication protocol-specific encryption of the data on the
4 first network node, and
5 b) performing a communication protocol-specific decryption of the data on the
6 second network node.

1 15. (Unamended) The computer data signal of Claim 13, wherein the first stream is a
2 first Java stream,
3 wherein the second stream is a second Java stream,
4 wherein the step of establishing a communication channel between the first and
5 second network nodes further comprises the step of establishing a Java secure
6 channel between the first and second network nodes,
7 wherein the step of establishing a first stream between the first process and the
8 communication channel further comprises the step of establishing a first Java
9 stream between the first process and the Java secure channel,
10 wherein the step of establishing a second stream between the second process and the
11 communication channel further comprises the step of establishing a second
12 Java stream between the second process and the Java secure channel,

13 wherein the step of writing the encrypted data to the first stream further comprises
14 the step of writing the encrypted data to the first Java stream, and
15 wherein the step of reading the encrypted data from the second stream further
16 comprises the step of reading the encrypted data from the second Java stream.

1 16. (Unamended) The computer data signal of Claim 13, wherein the communication
2 channel is a Java secure channel,
3 wherein the first stream is a Java stream,
4 wherein the second stream is a Java stream,
5 wherein the computer sequence of instructions further includes instructions for
6 connecting the Java secure channel to a third Java stream, and
7 wherein the third Java stream provides for the transmission of data according to a
8 specific communication protocol.

1 17. (Unamended) A method for providing communication protocol-independent security
2 for data transmitted by a process executing on a network node, the method
3 comprising the steps of:
4 a) establishing a stream between the process and a communication channel;
5 b) encrypting data to be transmitted by the process, the encrypting of the data
6 being independent of a communication protocol supported by the network
7 node;
8 c) writing the encrypted data to the stream; and
9 d) causing the encrypted data to be transmitted from the network node to the
10 communication channel.

1 18. (Unamended) The method of Claim 17, wherein the communication channel is a
2 Java secure channel,

3 wherein the stream is a first Java stream,
4 wherein the step of establishing a stream between the process and the communication
5 channel further comprises the step of establishing a Java stream between the
6 process and the Java secure channel, and
7 wherein the step of writing the encrypted data to the stream further comprises the
8 step of writing the encrypted data to the Java stream.

1 19. (Unamended) The method of Claim 17, wherein the communication channel is a
2 Java secure channel, wherein the stream is a Java stream,
3 wherein the method further comprises the step of connecting the Java secure channel
4 to a second Java stream, and
5 wherein the second Java stream provides for the transmission of data according to a
6 specific communication protocol.